UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,011	11/03/2003	Ralph E. Wesinger JR.	GRAPH-003COD	5849

28661 7590 05/18/2007
SIERRA PATENT GROUP, LTD.
1657 Hwy 395, Suite 202
Minden, NV 89423

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/18/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,011	WESINGER ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *20-38* is/are pending in the application.

4a) Of the above claim(s) *1-19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *20-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 20-38 remain pending.

Claims 1-19 are cancelled.

2. This is a Non-Final rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 20-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Civanlar, et al. (5,617,540) and Blackett, et al. (US 6,792,337), and in further view of Rosotoker, et al. (US 5,708,659).

As per claim 20:

Civanlar discloses a load-sharing server multi-homed firewall array comprising:

an array of [*firewall*] machines coupled in parallel with an IP-compliant network; **[col.1, lines 39-56]**

wherein each of the [*firewall*] machines of the array comprising:

a first and second set of virtual hosts, said first set of virtual hosts configured to interface an associated [*firewall*] machine [*with said IP-compliant network*] and said

second set of virtual hosts configured to interface an associated [*firewall*] machine [*with a private network*]; **[col.1, lines 56-66 and col.3, lines 2-6; Civanlar discusses virtual host's name which it is obvious that the virtual host's name is for a virtual host wherein corresponds to a server. Thus, the multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58).]**

each of said virtual hosts of said first and second set corresponding to a distinct home **[col.4, lines 39-40 and 60-61]** through which a connection may be made [*between said IP-compliant network and said private network*]; **[col.6, lines 23-25 and col.7, lines 54-62]**

DNS functionality associated with each of [*firewall*] machines of the array; **[col.1, lines 49-55]**

a master configuration file associated with each of the [*firewall*] machines; and **[col.6, lines 40-42 and col.7, lines 34-37]**

wherein an ensuing connection request is mapped to the first [*firewall*] machine of the array to respond to a DNS request associated with said ensuing connection request. **[col.5, lines 20-35 and col.5, line 66 – col.6, line 16]**

Civanlar discloses multimedia servers but did not go into details that the multimedia servers are intended to protect an organization's network against external threats coming from another network, which is known of a firewall. Thus, Civanlar did not include firewalls.

Blackett, et al. discloses a communications architecture that can be used for monitoring, protection, and control of devices and electrical power distribution in an electrical power distribution system (col.4, lines 60-63). Further, the architecture includes a communications network that is publicly accessible data network such as the Internet or other network or combination of sub-networks that transmit data utilizing the transmission control protocol/Internet protocol (TCP/IP) wherein such networks include private intranet networks, virtual private networks, extranets or combination that includes the Internet (col.6, lines 8-15). Blackett discloses all communications occurs securely via the network to ensure the received communications are authentic and has the ability to communication through network protection devices such as firewalls (col.7, lines 1-8). Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of multimedia servers with corresponding host names that are mapped by DNS tables by Civanlar to include firewalls as taught by Blackett because firewalls are protection devices that secures communications entering the network (Blackett-col.7, lines 1-8).

Civanlar discloses multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58). The claimed a distinct home is broad and can give more than one meaning as long as the virtual hosts correspond to a home. As such, a distinct home can broadly be given in light as the ATM switch or a multimedia service provider as disclosed in Civanlar. The servers 307 and 309 are connected to ATM switch 312 or servers 305 and 311 are connected to ATM switch 315 (col.4, lines 1-2). The multimedia servers 305, 307, 309, 311 are

operated by the multimedia service provider where each of the servers corresponds to a service provider (col.4, lines and 39-40 and 60-62). Therefore, Civanlar meets the limitation of the claimed each of said virtual hosts of said set corresponding to a distinct home. Civanlar discloses establishing communications with the (virtual hosts) multimedia servers that corresponds to the virtual host names and mapping the connections (col.3, lines 12-21 and col.5, line 66 – col.6, line 16). Blackett discloses firewalls are protection devices that secure communications entering the network. Although, the Civanlar and Blackett combination discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request. However, the connection request does not involve an IP-compliant network and a private network through which a connection may be made between said IP-compliant network and said private network.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker

discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of network connectivity by allowing connections to be established with the multimedia servers (virtual hosts) by Civanlar with the teaching of translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private network by Rosotoker because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different

network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

As per claim 21: See Civanlar on col.2, lines 39-43 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 20, wherein a connection request received from the IP-compliant network is mapped to said first set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 22: See Civanlar on col.4, lines 51-60 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 20, wherein a connection request received from the private network is mapped to said second set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 23: See Blackett on col.13, lines34-36; discussing load-sharing multi-homed firewall array of claim 20, wherein each of said firewall machines further comprises a special-purpose virtual host including an HTML-based configuration module for updating said master configuration files over said IP-compliant network.

As per claim 24: See Civanlar on col.1, lines 17-19 and Blackett on col.2, lines 1-6; discussing load-sharing multi-homed firewall array of claim 23, wherein each of said firewall machines includes N + 1 sets of virtual hosts.

As per claim 25:

Civanlar discloses a load-sharing multi-homed [*firewall*] array comprising:

means for coupling a plurality of [*firewall*] means in parallel with an IP-compliant network; **[col.1, lines 39-56]**

wherein each of said [*firewall*] means comprising:

a first set of virtual host means interfacing an associated [*firewall*] means [*with said IP-compliant network*] and said second set of virtual host means interfacing an associated [*firewall*] means [*with a private network*]; **[col.1, lines 56-66 and col.3, lines 2-6; Civanlar discusses virtual host's name which it is obvious that the virtual host's name is for a virtual host wherein corresponds to a server. Thus, the multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58).]**

each of said virtual hosts of said first and second set corresponding to a distinct home **[col.4, lines 39-40 and 60-61]** through which a connection may be made [*between said IP-compliant network and said private network*]; **[col.6, lines 23-25 and col.7, lines 54-62]**

means for providing DNS functionality associated with each of [*firewall*] means; **[col.1, lines 49-55]**

master configuration means associated with each of the [*firewall*] machines; and **[col.6, lines 40-42 and col.7, lines 34-37]**

means for mapping an ensuing connection request to the first [*firewall*] means to respond to a DNS request associated with said ensuing connection request. **[col.5, lines 20-35 and col.5, line 66 – col.6, line 16]**

Civanlar discloses multimedia servers but did not go into details that the multimedia servers are intended to protect an organization's network against external threats coming from another network, which is known of a firewall. Thus, Civanlar did not include firewalls.

Blackett, et al. discloses a communications architecture that can be used for monitoring, protection, and control of devices and electrical power distribution in an electrical power distribution system (col.4, lines 60-63). Further, the architecture includes a communications network that is publicly accessible data network such as the Internet or other network or combination of sub-networks that transmit data utilizing the transmission control protocol/Internet protocol (TCP/IP) wherein such networks include private intranet networks, virtual private networks, extranets or combination that includes the Internet (col.6, lines 8-15). Blackett discloses all communications occurs securely via the network to ensure the received communications are authentic and has the ability to communication through network protection devices such as firewalls (col.7, lines 1-8). Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of multimedia servers with corresponding host names that are mapped by DNS tables by Civanlar to include firewalls as taught by Blackett because firewalls are protection devices that secures communications entering the network (Blackett-col.7, lines 1-8).

Civanlar discloses multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58). The claimed a distinct home is broad and can give more than one meaning as long as the virtual hosts correspond to a home. As such, a distinct home can broadly be given in light as the ATM switch or a multimedia service provider as disclosed in Civanlar. The servers 307 and 309 are connected to ATM switch 312 or servers 305 and 311 are connected to ATM switch 315 (col.4, lines 1-2). The multimedia servers 305, 307, 309, 311 are

operated by the multimedia service provider where each of the servers corresponds to a service provider (col.4, lines and 39-40 and 60-62). Therefore, Civanlar meets the limitation of the claimed each of said virtual hosts of said set corresponding to a distinct home. Civanlar discloses establishing communications with the (virtual hosts) multimedia servers that corresponds to the virtual host names and mapping the connections (col.3, lines 12-21 and col.5, line 66 – col.6, line 16). Blackett discloses firewalls are protection devices that secure communications entering the network. Although, the Civanlar and Blackett combination discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request. However, the connection request does not involve an IP-compliant network and a private network through which a connection may be made between said IP-compliant network and said private network.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker

discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of network connectivity by allowing connections to be established with the multimedia servers (virtual hosts) by Civanlar with the teaching of translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private network by Rosotoker because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different

network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

As per claim 26: See Civanlar on col.2, lines 39-43 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 25, further comprising means for mapping a connection request received from the IP-compliant network to said first set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 27: See Civanlar on col.4, lines 51-60 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 25, further comprising means for mapping a connection request received from the private network to said second set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 28: See Blackett on col.13, lines34-36; discussing load-sharing multi-homed firewall array of claim 25, further comprising HTML-based configuration means for updating said master configuration means over said IP-compliant network.

As per claim 29: See Civanlar on col.1, lines 17-19 and Blackett on col.2, lines 1-6; discussing load-sharing multi-homed firewall array of claim 28, wherein each of said firewall means includes N + 1 sets of virtual host means.

As per claim 30:

Civanlar discloses a load-sharing multi-homed [*firewall*]array comprising:

an array of [*firewall*] machines coupled in a parallel with an IP-compliant network; **[col.1, lines 39-56]**

wherein each of the [*firewall*] machines of the array comprising:

at least a first and second set of virtual hosts, said first set of virtual hosts configured to interface an associated [*firewall*] machine [*with said IP-compliant network*] and said second set of virtual hosts configured to interface an associated [*firewall*] machine [*with a private network*]; **[col.1, lines 56-66 and col.3, lines 2-6; Civanlar discusses virtual host's name which it is obvious that the virtual host's name is for a virtual host wherein corresponds to a server. Thus, the multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58).]**

DNS functionality associated with each of [*firewall*] machines of the array; **[col.1, lines 49-55]**

a master configuration file associated with each of the [*firewall*] machines; **[col.6, lines 40-42 and col.7, lines 34-37]**

a special-purpose virtual host including [*an HTML-based*] configuration module for updating said master configuration files **[col.2, lines 30-35 and col.6, lines 40-42]** using a point-and-click interface over said IP-compliant network; and **[col.1, lines 52-55 and col.9, lines 50-65]**

wherein an ensuing connection request is mapped to the first [*firewall*] machine of the array to respond to a DNS request associated with said ensuing connection request. **[col.5, lines 20-35 and col.5, line 66 – col.6, line 16]**

However, Civanlar did not include firewall machines and HTML-based configuration module.

Blackett, et al. discloses a communications architecture that can be used for monitoring, protection, and control of devices and electrical power distribution in an electrical power distribution system (col.4, lines 60-63). Further, the architecture includes a communications network that is publicly accessible data network such as the Internet or other network or combination of sub-networks that transmit data utilizing the transmission control protocol/Internet protocol (TCP/IP) wherein such networks include private intranet networks, virtual private networks, extranets (col.6, lines 8-15) and the computer executing a web/HTML browser program such as the Internet that can be readily accessible format once converted (col.13, lines 34-36 and col.16, lines 11-15). Blackett discloses all communications occurs securely via the network to ensure the received communications are authentic and has the ability to communication through network protection devices such as firewalls (col.7, lines 1-8). Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of multimedia servers with corresponding host names that are mapped by DNS tables by Civanlar to include firewalls and HTML-based configuration module as taught by Blackett because firewalls are protection devices that secures communications entering the network (Blackett-col.7, lines 1-8) and HTML is more readily accessible format once the received data is converted to HTML (Blackett-col.16, lines 11-15).

Civanlar discloses multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58). The claimed a distinct home is broad and can give more than one meaning as long as the virtual hosts

correspond to a home. As such, a distinct home can broadly be given in light as the ATM switch or a multimedia service provider as disclosed in Civanlar. The servers 307 and 309 are connected to ATM switch 312 or servers 305 and 311 are connected to ATM switch 315 (col.4, lines 1-2). The multimedia servers 305, 307, 309, 311 are operated by the multimedia service provider where each of the servers corresponds to a service provider (col.4, lines and 39-40 and 60-62). Therefore, Civanlar meets the limitation of the claimed each of said virtual hosts of said set corresponding to a distinct home. Civanlar discloses establishing communications with the (virtual hosts) multimedia servers that corresponds to the virtual host names and mapping the connections (col.3, lines 12-21 and col.5, line 66 – col.6, line 16). Blackett discloses firewalls are protection devices that secure communications entering the network. Although, the Civanlar and Blackett combination discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request. However, does not involve an IP-compliant network and a private network associated with ensuing connection request that is mapped to respond to a DNS request.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26). Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing

system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of network connectivity by allowing connections to be established with the multimedia servers (virtual hosts) by Civanlar with the teaching of translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private

network by Rosotoker because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

As per claim 31: See Civanlar on col.2, lines 39-43 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 30, wherein: connection request received from the IP-compliant network is mapped to said first set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 32: See Civanlar on col.4, lines 51-60 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 30, wherein connection request received from the private network is mapped to said second set of virtual hosts on the first firewall machine of the array to respond to a DNS request.

As per claim 33: See Blackett on col.13, lines34-36; discussing load-sharing multi-homed firewall array of claim 30, wherein each of said firewall machines further comprises a special-purpose virtual host including an HTML-based configuration module for updating said master configuration files over said IP-compliant network.

As per claim 34: See Civanlar on col.1, lines 17-19 and Blackett on col.2, lines 1-6; discussing load-sharing multi-homed firewall array of claim 33, wherein each of said firewall machines includes N + 1 sets of virtual hosts.

As per claim 35:

Civanlar discloses a load-sharing multi-homed [*firewall*] array comprising:

means for coupling a plurality of [*firewall*] means in parallel with an IP-compliant network; **[col.1, lines 39-56]**

wherein each of said [*firewall*] means comprising:

a first set of virtual host means interfacing an associated [*firewall*] means [*with said IP-compliant network*] and said second set of virtual host means interfacing an associated [*firewall*] machine [*with a private network*]; **[col.1, lines 56-66 and col.3, lines 2-6; Civanlar discusses virtual host's name which it is obvious that the virtual host's name is for a virtual host wherein corresponds to a server. Thus, the multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58).]**

means for providing DNS functionality associated with each of [*firewall*] means; **[col.1, lines 49-55]**

master configuration means associated with each of the [*firewall*] machines; **[col.6, lines 40-42 and col.7, lines 34-37]**

[*an HTML-based*] configuration means for updating said master configuration means **[col.2, lines 30-35 and col.6, lines 40-42]** using a point-and-click interface over said IP-compliant network; and **[col.1, lines 52-55 and col.9, lines 50-65]**

means for mapping an ensuing connection request to the first [*firewall*] means to respond to a DNS request associated with said ensuing connection request. **[col.5, lines 20-35 and col.5, line 66 – col.6, line 16]**

However, Civanlar did not include firewall machines and HTML-based configuration means.

Blackett, et al. discloses a communications architecture that can be used for monitoring, protection, and control of devices and electrical power distribution in an electrical power distribution system (col.4, lines 60-63). Further, the architecture includes a communications network that is publicly accessible data network such as the Internet or other network or combination of sub-networks that transmit data utilizing the transmission control protocol/Internet protocol (TCP/IP) wherein such networks include private intranet networks, virtual private networks, extranets (col.6, lines 8-15) and the computer executing a web/HTML browser program such as the Internet that can be readily accessible format once converted (col.13, lines 34-36 and col.16, lines 11-15). Blackett discloses all communications occurs securely via the network to ensure the received communications are authentic and has the ability to communication through network protection devices such as firewalls (col.7, lines 1-8). Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of multimedia servers with corresponding host names that are mapped by DNS tables by Civanlar to include firewalls and HTML-based configuration module as taught by Blackett because firewalls are protection devices that secures communications entering the network (Blackett-col.7, lines 1-8) and HTML is more readily accessible format once the received data is converted to HTML (Blackett-col.16, lines 11-15).

Civanlar discloses multimedia servers with corresponding virtual hosts names are the claimed set of virtual hosts (col.4, lines 42-45 and 57-58). The claimed a distinct home is broad and can give more than one meaning as long as the virtual hosts correspond to a home. As such, a distinct home can broadly be given in light as the ATM switch or a multimedia service provider as disclosed in Civanlar. The servers 307 and 309 are connected to ATM switch 312 or servers 305 and 311 are connected to ATM switch 315 (col.4, lines 1-2). The multimedia servers 305, 307, 309, 311 are operated by the multimedia service provider where each of the servers corresponds to a service provider (col.4, lines and 39-40 and 60-62). Therefore, Civanlar meets the limitation of the claimed each of said virtual hosts of said set corresponding to a distinct home. Civanlar discloses establishing communications with the (virtual hosts) multimedia servers that corresponds to the virtual host names and mapping the connections (col.3, lines 12-21 and col.5, line 66 – col.6, line 16). Blackett discloses firewalls are protection devices that secure communications entering the network. Although, the Civanlar and Blackett combination discloses virtual hosts and ensuing connection request is mapped to the firewall machine of the array to respond to a DNS request associated with said ensuing connection request. However does not involve an IP-compliant network and a private network associated with ensuing connection request that is mapped to respond to a DNS request.

Rosotoker discloses network technology has suffered from limitations resulting from a proliferation of non-standard protocols, and limitations due to the nature of the protocols and transmission schemes, which are employed (col.2, lines 22-26).

Rosotoker discloses that under heavy traffic, any attempt to determine to which port a packet must be switched must be accomplished speedily to avoid slowing throughput of the network (col.2, lines 41-45). Rosotoker discusses the network protocol processing system interconnection comprises packet conversion logic for conversion between network protocol (col.4, line 66 – col.5, line 1) where the invention is not necessarily limited to the particular protocols and standards used (col.25, lines 45-52). Rosotoker discusses the remote node connections typically exchange packets of data in Novell IPX, Microsoft NetBEUI, or Internet IP format (col.7, lines 65-67). Thus, depending upon the protocol employed internally the data received over a particular port may require translation from one protocol to another (col.18, lines 5-10) obviously suggests the received IP-compliant traffic being destined for said non-IP compliant destination. Further, Rosotoker discloses translating incoming packets in any protocol and outgoing packets in any different protocol (col.9, lines 28-31). Rosotoker discusses the ATM protocol is preferred but can use other protocols (col.8, lines 55-58). Rosotoker teaches the conversion between a network protocol (i.e. IP-compliant) and the data protocol (i.e. non-IP compliant) used to handle large data streams such as MPEG packets but not limited to these particular protocols (col.25, lines 44-53). By translating outgoing packets in any protocol obviously can transform the IP-compliant traffic into a non-IP protocol appropriate for a destination. Hence, Rosotoker obviously suggests an IP-compliant network and a private network through which a connection may be made.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of network connectivity by allowing connections to be established

with the multimedia servers (virtual hosts) by Civanlar with the teaching of translation/conversion from one protocol to another (Rosotoker - col.18, lines 5-10) through which a connection may be made between said IP-compliant network and said private network by Rosotoker because translating to a different protocol can accommodate the data stream of a non-IP compliant destination and providing connections to different network protocols to provide multiple external communication port connections transparent to the destined (Rosotoker-col.25, lines 34-37 and 44-52).

As per claim 36: See Civanlar on col.2, lines 39-43 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 35, further comprising means for mapping a connection request received from the IP-compliant network to said first set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 37: See Civanlar on col.4, lines 51-60 and col.5, lines 20-35; discussing load-sharing multi-homed firewall array of claim 35, further comprising means for mapping a connection request received from the private network to said second set of virtual host means on the first firewall means to respond to a DNS request.

As per claim 38: See Civanlar on col.1, lines 17-19 and Blackett on col.2, lines 1-6; discussing load-sharing multi-homed firewall array of claim 35, wherein each of said firewall means includes N + 1 sets of virtual host means.

Response to Arguments

4. Applicant's arguments, filed 3/2/2007, with respect to the rejection(s) of claim(s) 20-38 under Double Patenting have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Civanlar, et al. (5,617,540) and Blackett, et al. (US 6,792,337), and in further view of Rosotoker, et al. (US 5,708,659).

Applicant's terminal disclosure have been approved and entered on 3/7/2007. However, upon an updated search, the examiner found prior art to support the claimed invention. Therefore, claims 20-38 remains rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100